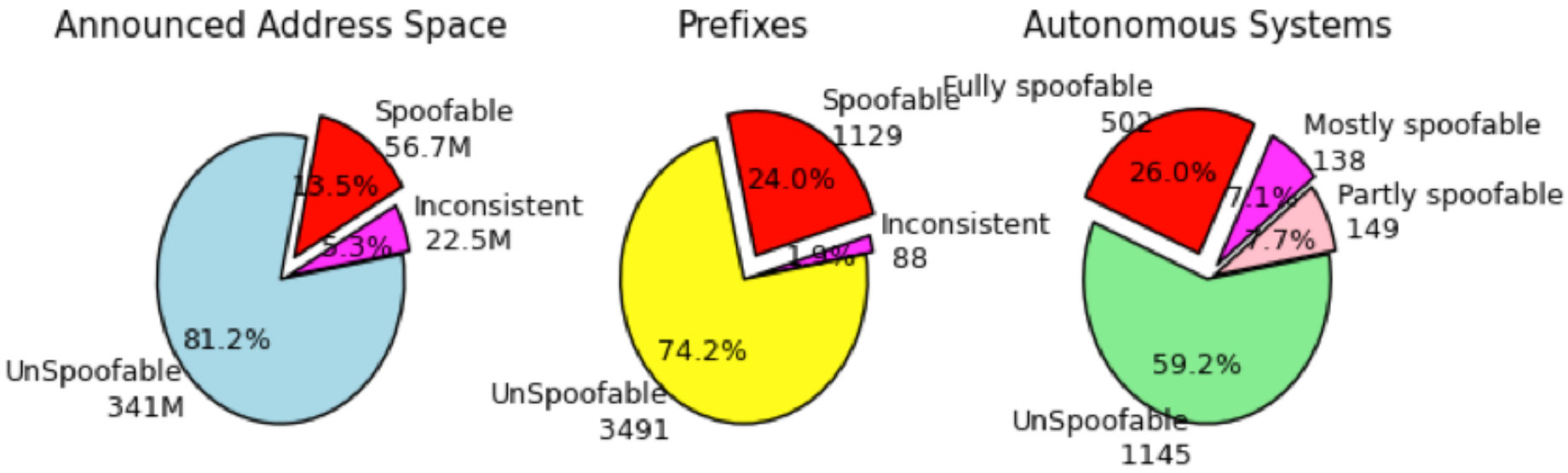
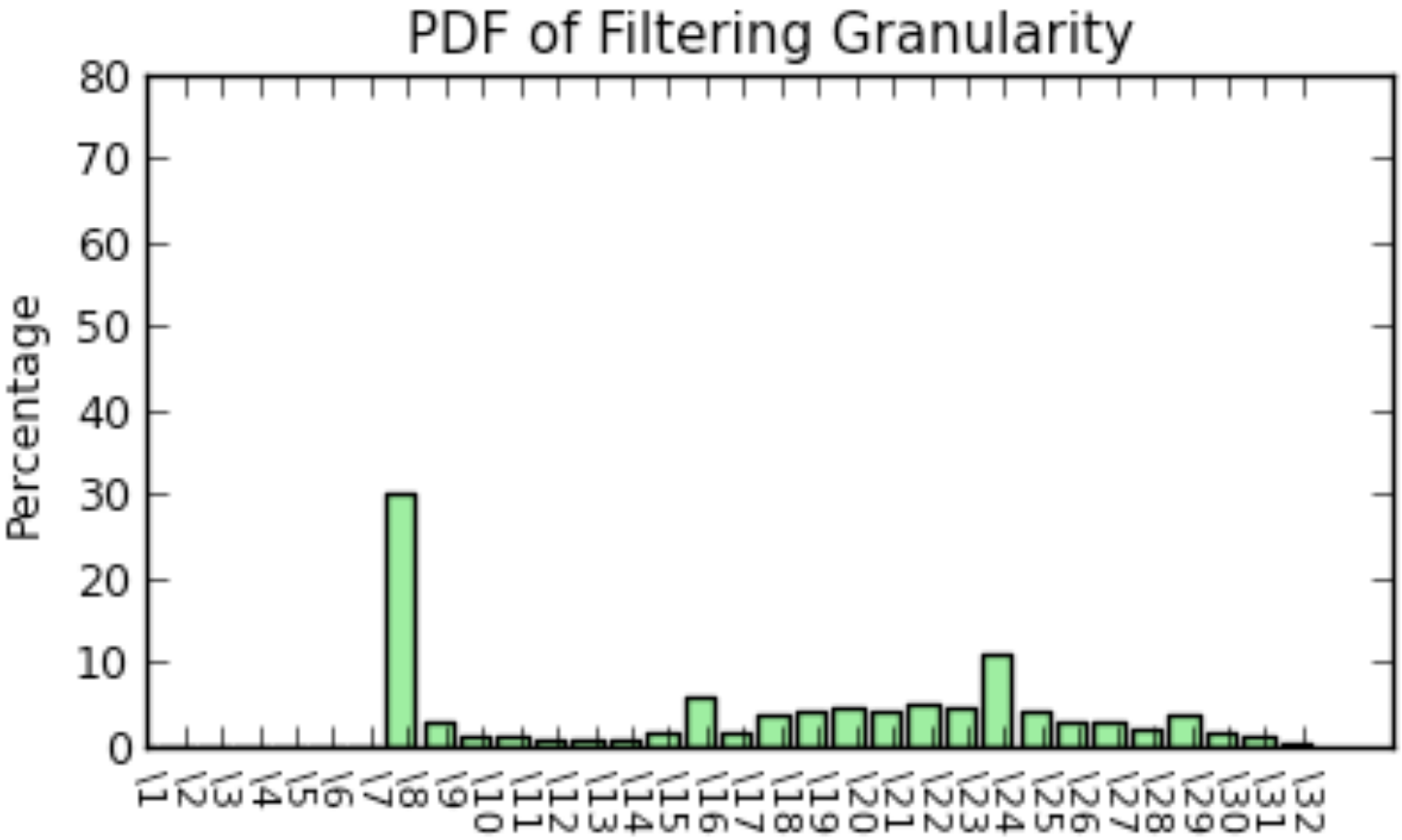
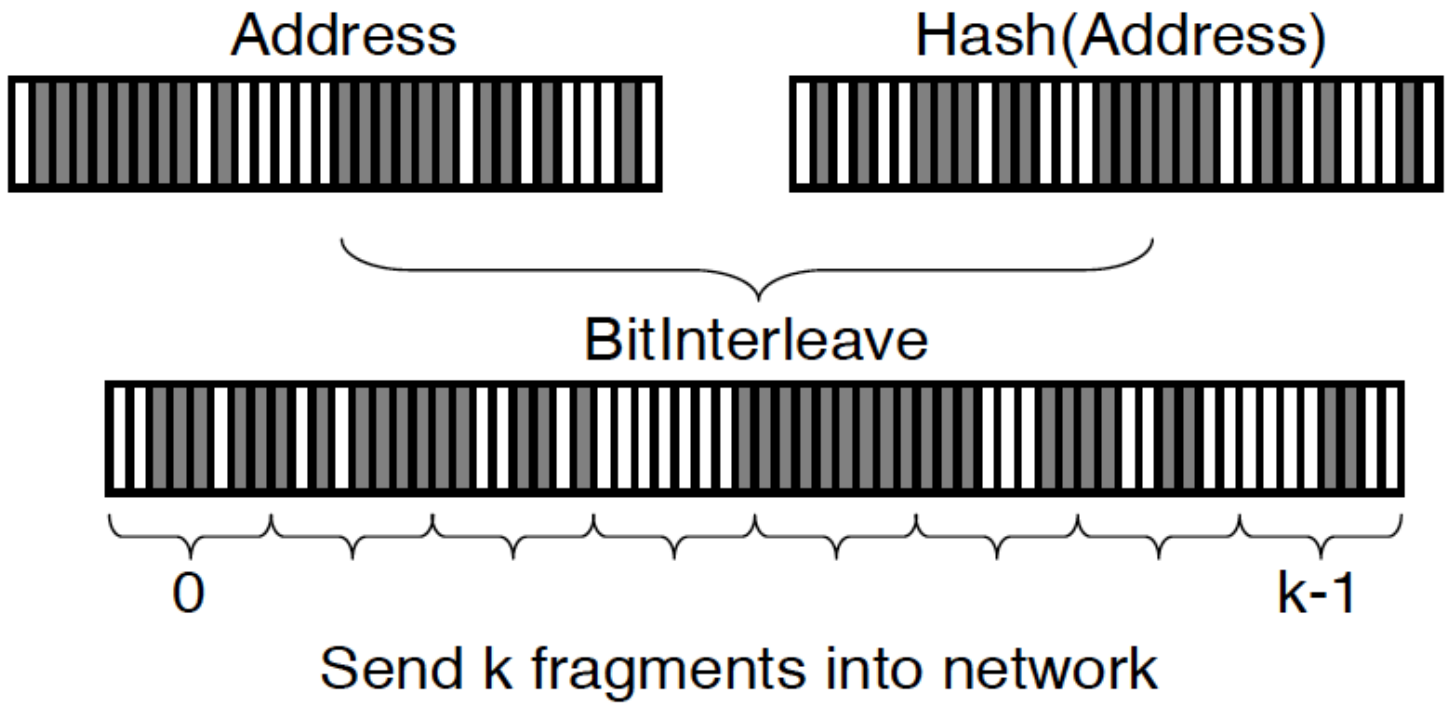
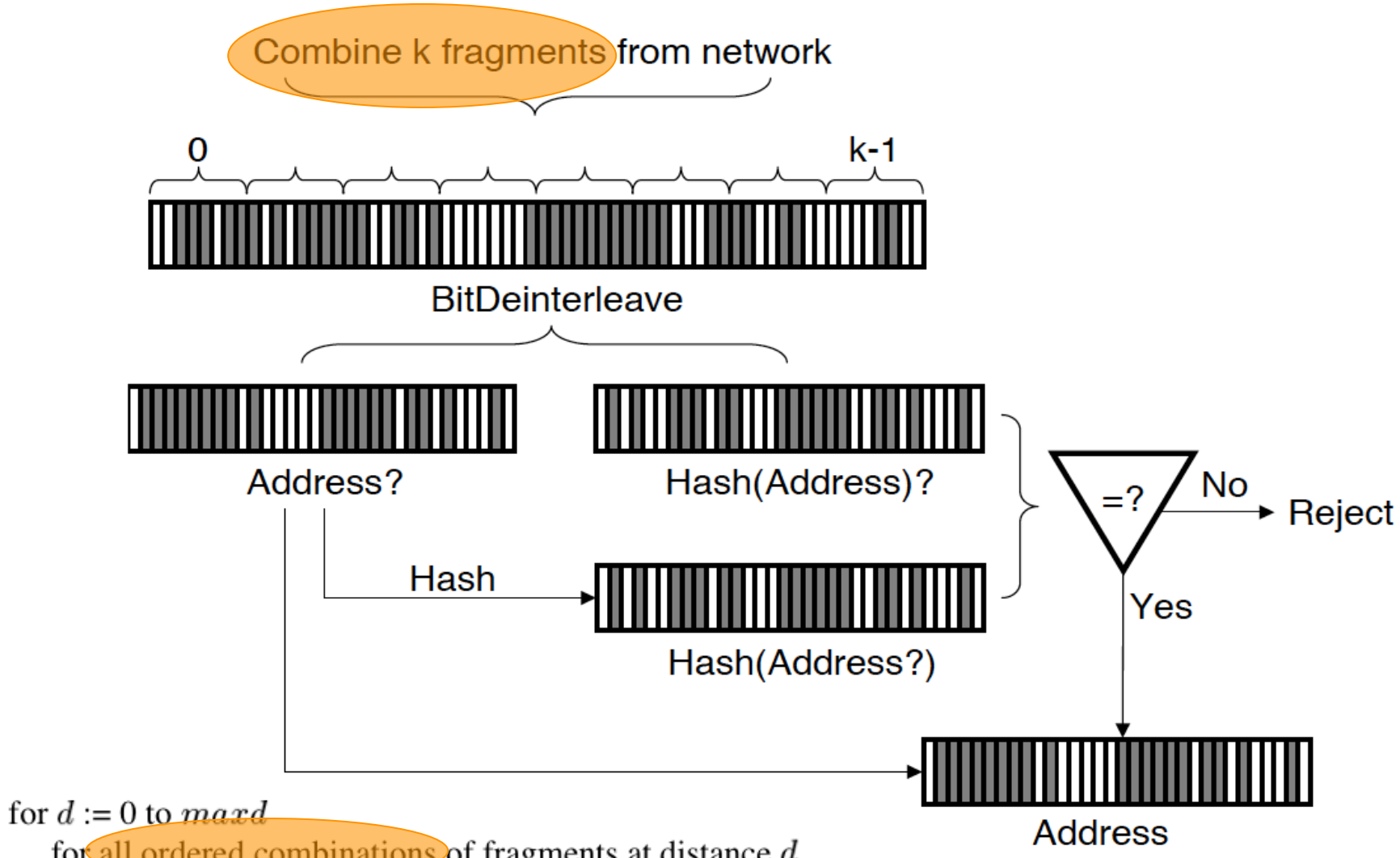
Data Range: *Fri Feb 11 08:16:52 EST 2005 to Wed Sep 17 12:45:40 EDT 2014*
Total Tests: *22907*
Unique IPs tested: *18193*
Unique Routed Prefixes tested from: *9874*
Unique ASes tested from: *3099*




PDF of Filtering Granularity
Percentage
80
70
60
50
40
30
20
10
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

We define the *approximate trace-back* problem as finding a candidate attack path for each attacker that contains the true attack path as a suffix. We call this the *valid suffix* of the candidate path.


Address
Hash(Address)
BitInterleave
0
k-1
Send k fragments into network



for $d := 0$ to $maxd$
  for all ordered combinations of fragments at distance d
    construct edge z
    if $d \neq 0$ then
      $z := z \oplus last$
    if Hash(EvenBits(z)) = OddBits(z) then
      insert edge (z,EvenBits(z),d) into G
      $last$:= EvenBits(z);

	Management overhead	Network overhead	Router overhead	Distributed capability	Post-mortem capability	Preventative/ reactive
Ingress filtering	Moderate	Low	Moderate	N/A	N/A	Preventative
Link testing						
Input debugging	High	Low	High	Good	Poor	Reactive
Controlled flooding	Low	High	Low	Poor	Poor	Reactive
Logging	High	Low	High	Excellent	Excellent	Reactive
ICMP Traceback	Low	Low	Low	Good	Excellent	Reactive
Marking	Low	Low	Low	Good	Excellent	Reactive

Table 1: Qualitative comparison of existing schemes for combating anonymous attacks and the probabilistic marking approach we propose.

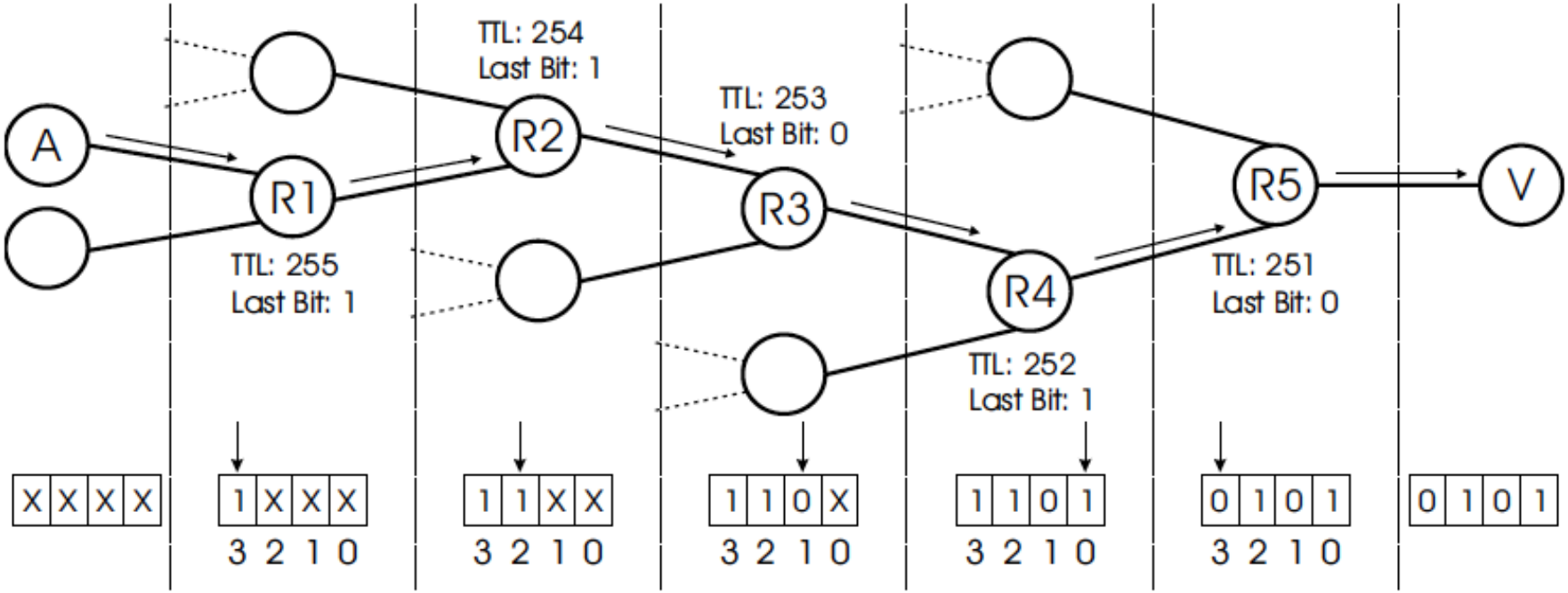
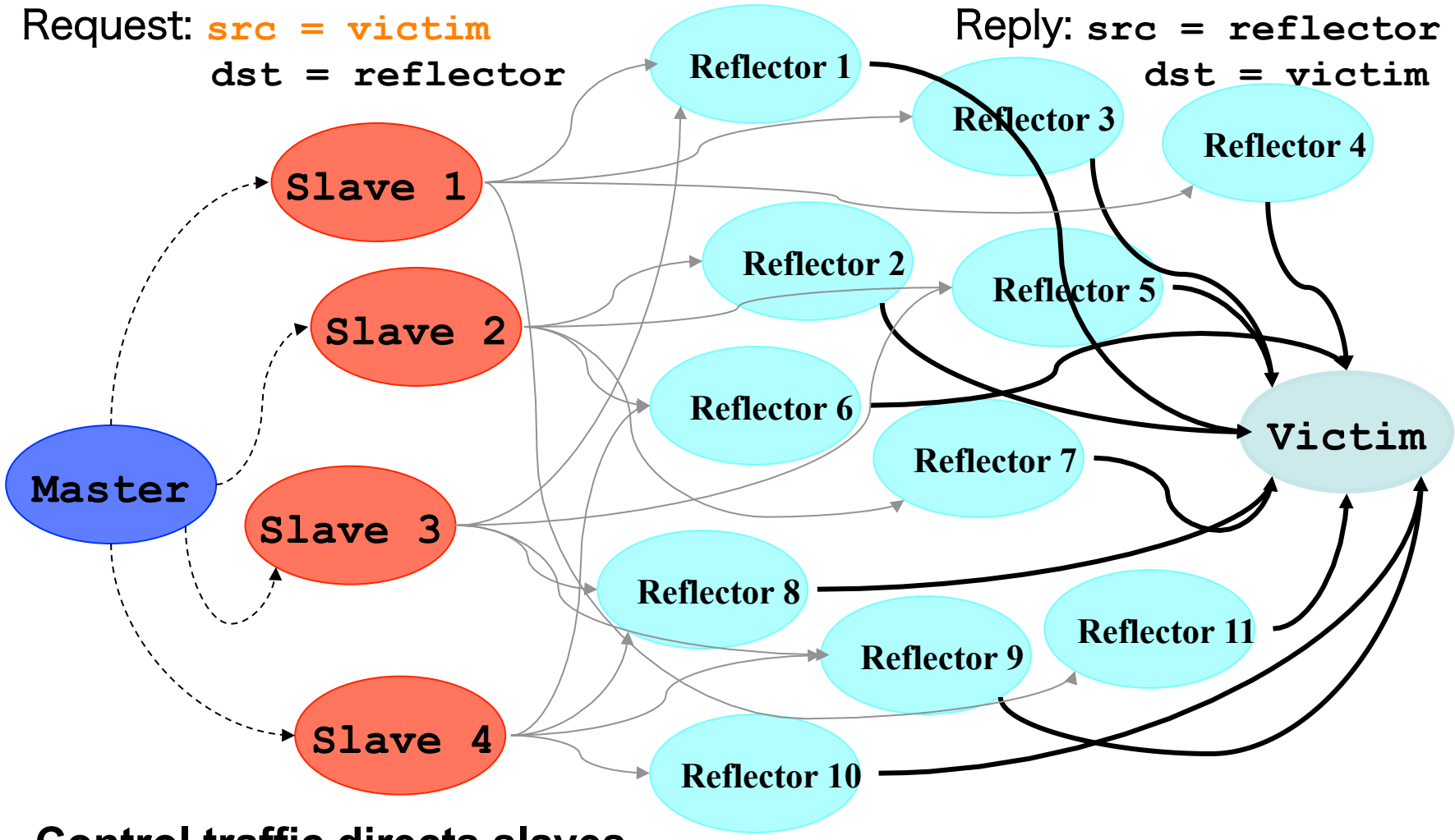


Figure 3. Example of our initial marking scheme. The packet travels from the attacker A to the victim V across the routers R1 to R5. Each router uses the TTL value of the packet to index into the IP identification field to insert its marking. In this example we show a 1-bit marking in a 4-bit field for simplicity.

```
cory 1 % ping -s 128.32.48.0
PING 128.32.48.0: 56 data bytes
```

```
cory 1 % ping -s 128.32.48.0
PING 128.32.48.0: 56 data bytes
64 bytes from cory.EECS.Berkeley.EDU (128.32.48.187): icmp_seq=0. time=0.599 ms
64 bytes from verify.EECS.Berkeley.EDU (128.32.48.124): icmp_seq=0. time=1.66 ms
64 bytes from claude.EECS.Berkeley.EDU (128.32.48.242): icmp_seq=0. time=3.50 ms
64 bytes from wiener.EECS.Berkeley.EDU (128.32.48.173): icmp_seq=0. time=4.89 ms
64 bytes from cronus-48.CS.Berkeley.EDU (128.32.48.21): icmp_seq=0. time=6.24 ms
64 bytes from skyros.EECS.Berkeley.EDU (128.32.48.189): icmp_seq=0. time=7.60 ms
64 bytes from citrissrv4.EECS.Berkeley.EDU (128.32.48.138): icmp_seq=0. time=8.95 ms
64 bytes from kea.EECS.Berkeley.EDU (128.32.48.161): icmp_seq=0. time=10.3 ms
64 bytes from rhea-48.CS.Berkeley.EDU (128.32.48.23): icmp_seq=0. time=11.7 ms
64 bytes from mercury2.EECS.Berkeley.EDU (128.32.48.116): icmp_seq=0. time=13.1 ms
64 bytes from transacct.EECS.Berkeley.EDU (128.32.48.243): icmp_seq=0. time=14.4 ms
64 bytes from erso-stag.EECS.Berkeley.EDU (128.32.48.235): icmp_seq=0. time=15.8 ms
64 bytes from pems-pl.EECS.Berkeley.EDU (128.32.48.206): icmp_seq=0. time=17.1 ms
64 bytes from pemsdc.EECS.Berkeley.EDU (128.32.48.199): icmp_seq=0. time=18.4 ms
64 bytes from pemscs.EECS.Berkeley.EDU (128.32.48.156): icmp_seq=0. time=19.8 ms
64 bytes from erso-dev.EECS.Berkeley.EDU (128.32.48.188): icmp_seq=0. time=21.1 ms
64 bytes from kynthos.EECS.Berkeley.EDU (128.32.48.125): icmp_seq=0. time=22.6 ms
64 bytes from pemsdb.EECS.Berkeley.EDU (128.32.48.157): icmp_seq=0. time=24.1 ms
64 bytes from ildap2.EECS.Berkeley.EDU (128.32.48.164): icmp_seq=0. time=25.5 ms
64 bytes from pulsar.EECS.Berkeley.EDU (128.32.48.149): icmp_seq=0. time=26.8 ms
64 bytes from quasar.EECS.Berkeley.EDU (128.32.48.145): icmp_seq=0. time=28.2 ms
64 bytes from c199.EECS.Berkeley.EDU (128.32.48.169): icmp_seq=0. time=29.6 ms
64 bytes from boron.EECS.Berkeley.EDU (128.32.48.118): icmp_seq=0. time=31.0 ms
64 bytes from silicon2.EECS.Berkeley.EDU (128.32.48.204): icmp_seq=0. time=32.4 ms
64 bytes from print199md-cc.EECS.Berkeley.EDU (128.32.48.196): icmp_seq=0. time=33.8 ms
64 bytes from silicon.EECS.Berkeley.EDU (128.32.48.237): icmp_seq=0. time=35.2 ms
64 bytes from print197m.EECS.Berkeley.EDU (128.32.48.227): icmp_seq=0. time=36.6 ms
64 bytes from print144ma.EECS.Berkeley.EDU (128.32.48.228): icmp_seq=0. time=38.0 ms
64 bytes from cory115-1-gw.EECS.Berkeley.EDU (128.32.48.1): icmp_seq=0. time=39.4 ms
64 bytes from print199ma.EECS.Berkeley.EDU (128.32.48.201): icmp_seq=0. time=40.8 ms
64 bytes from print199mb.EECS.Berkeley.EDU (128.32.48.202): icmp_seq=0. time=42.2 ms
```

Diffuse DDoS: Reflector Attack



Control traffic directs slaves at victim & reflectors

Reflectors send streams of non-spoofed but unsolicited traffic to victim